UNITED STATES PATENT APPLICATION

FOR

METHOD AND APPARATUS FOR VIRTUAL PRIVATE NETWORKS

Inventors:

Hamid Asayesh
Gerald Neufeld
Rene Tio

Prepared by:

Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Blvd., Suite 700
Los Angeles, California 90025
(410) 207-3800

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number: **EL 485753676US** Date of Deposit: **August 28, 2001**

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Commissioner of Patents and Trademarks, Washington, D. C. 20241

Shenise Ramdeen
(Typed or printed name of person mailing paper or fee)

Shenise Ramdeen
(Signature of person mailing paper or fee)

8-28-01
(Date signed)

METHOD AND APPARATUS FOR VIRTUAL PRIVATE NETWORKS

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The invention relates to the field of communication. More specifically, the invention relates to communication networks.

Background of the Invention

[0002] Virtual Private Networks (VPNs) extend an entity's (e.g., a corporation, Internet Service Provider (ISP), etc.) network backbone out to the Internet. The connectivity costs for VPNs are less than leasing a line and fault tolerance is improved because of multiple pathways between sites. Instead of an entity purchasing, administrating and maintaining additional network elements (e.g. routers, hubs, switches, subscriber management systems, etc.), an entity can securely transmit traffic through the Internet with VPNs. Corporations seek to extend their corporate networks to enable their telecommuters and individual offices to function as a single secure network. ISPs employ VPNs to extend their networks to maintain control of their subscribers at lower costs.

[0003] Unfortunately, VPNs are implemented with costly protocols, such as IPSec and MPLS. The addition of edge devices or routers requires configuration on more than just the endpoints of the VPN to support such VPNs. The intermediate network elements also require configuration. These administrative costs slow the process of adding equipment and/or adding VPNs. In addition, supporting VPNs implemented with these protocols also becomes costly.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] The invention may best be understood by referring to the following description and accompanying drawings that are used to illustrate embodiments of the invention. In the drawings:

[0005] Figure 1A is a diagram illustrating an exemplary network according to one embodiment of the invention.

[0006] Figure 1B is a diagram illustrating the network element 105 establishing a generic routing encapsulation virtual private network (GRE VPN) according to one embodiment of the invention.

[0007] Figure 1C is a diagram illustrating dynamic establishment of the GRE VPN according to one embodiment of the invention.

[0008] Figure 1D is a diagram illustrating traffic being transmitted over the GRE VPN according to one embodiment of the invention.

[0009] Figure 1E is a diagram illustrating multiple VPNs over a single GRE tunnel according to one embodiment of the invention.

[0010] Figure 2 is a diagram illustrating the network element 105 according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE DRAWINGS

[0011] In the following description, numerous specific details are set forth to provide a thorough understanding of the invention. However, it is understood that the invention may be practiced without these specific details. In other instances, well-known circuits, structures, standards, and techniques have not been shown in detail in order not to obscure the invention.

[0012] Figure 1A is a diagram illustrating an exemplary network according to one embodiment of the invention. In Figure 1A, a site for company A 101 and a site for company B 103 are coupled with a network element 105. The sites 101 and 103 can be main offices, branch offices, etc. The network element 105 is coupled with a network

element 109 via a network cloud 107. The network element 109 is coupled with a second site for 111 company A and a second site for 113 company B . The network element 105 receives traffic from the company A site 101 and the company B site 103 and transmits the traffic through the network cloud 107 to the network element 109. The network element 105 also receives traffic from the network element 109 through the network cloud 107 and directs the traffic to the company A site 101 and the company B site 103 appropriately. Likewise, the network element 109 receives traffic from the company A site 111 and the company B site 113 and transmits the traffic through the network cloud 107 to the network element 105. The network element 109 also directs traffic received through the network cloud 107 to the company A site 111 and the company B site 113 appropriately.

[0013] Figure 1B is a diagram illustrating the network element 105 establishing a generic routing encapsulation virtual private network (GRE VPN) according to one embodiment of the invention. In Figure 1B, the network element 105 hosts virtual routers 115, 117, and 119. The virtual router 115 is configured for company A. The virtual router 117 is configured for company B . Traffic received from the company A site 101 by the network element 105 is processed by the virtual router 115. In this example, traffic 131 is received by the network element 105 from the company A site 101. The traffic 131 indicates a tunnel. The network element 105 queries a remote access dial-up server (RADIUS) 121 with the GRE tunnel name. The RADIUS 121 returns a set of endpoints for the GRE tunnel. In this example, the set of endpoints are network addresses that correspond to the network element 105 and the network element 109. After receiving a set of endpoints from the RADIUS 121, the network element 105 makes a second query to the RADIUS 121 with the set of endpoints and a key corresponding to the company A. The RADIUS 121 returns to the network element 105 a second set of endpoints corresponding to company A.

[0014] In an alternative embodiment, the sets of endpoints are stored on the network element 105 instead of 121. In another embodiment of the invention, the set of endpoints are stored on a network storage device coupled with the network element 105. In this example, one of the first set of endpoints is the Internet Protocol (IP) address corresponding to the virtual router 119 while one of the second set of endpoints is the IP address of the virtual router 115. The set of endpoints can be implemented as MAC

addresses, ATM circuit identifiers, etc. The virtual router 119 can be a virtual backbone router, a virtual local router, etc., for the network element 105.

[0015] The network element uses the first and second set of endpoints to configure an interface of the virtual router 115 to an interface of the virtual router 119. The network element 105 transmits the key for company A and the first set of endpoints, which include the IP address for the virtual router 119 and the IP address for the termination point of the GRE tunnel, to the termination point. In the described example, the termination point of the GRE tunnel is the network element 109.

[0016] Figure 1C is a diagram illustrating dynamic establishment of the GRE VPN according to one embodiment of the invention. In Figure 1C, the network element 109 hosts virtual routers 123, 125, and 127. The virtual router 123 could be configured as a backbone router, a local router, etc. The virtual router 125 is configured for company A. The virtual router 127 is configured for company B. The network element 109 receives the traffic transmitted from the network element 105 that includes the first set of endpoints for the GRE tunnel and the key for company A. The network element 109 queries the RADIUS 121 with the first set of endpoints and the key. The RADIUS 121 returns the second set of endpoints to the network element 109. In alternative embodiments, the second set of endpoints could be stored locally, in a network storage device, or a different RADIUS. In this example, a second one of the second set of endpoints is the IP address for the virtual router 125 while the second one of the first set of endpoints is the IP address for the virtual router 123. The network element 109 configures an interface of the virtual router 125 to an interface of the virtual router 123. The virtual router 123 receives the traffic 131 for the company A site 111 from the network element 105 and forwards the traffic to the virtual router 125.

[0017] Figure 1D is a diagram illustrating traffic being transmitted over a GRE VPN according to one embodiment of the invention. In Figure 1D, a generic routing encapsulation (GRE) tunnel 129 has been established between the network element 105 and the network element 109 through a network cloud 107. The company A site 101 can securely transmit traffic 131 to the company A site 111 via the GRE tunnel 129.

[0018] Figure 1E is a diagram illustrating multiple VPNs over a single GRE tunnel according to one embodiment of the invention. In Figure 1E, the company B site 103 is

transmitting traffic to the company B site 113. The traffic 131 from company A site 101 and the traffic 133 from company B site 103 both traverse the GRE tunnel 129. Provisioning multiple VPNs per tunnel results in fewer interfaces being configured and fewer addresses being required. At the network element 105, the traffic 131 and the traffic 133 are multiplexed into a traffic 135. The multiplexed traffic 135 traverses the GRE tunnel 129 and enters the network element 109. At the network element 109, the keys indicated in the multiplexed traffic 135 are used to de-multiplex the traffic 135 into the traffic 131 and the traffic 133. The traffic 131 and the traffic 133 are forwarded to the company A site 111 and the company B site 113 respectively.

[0019] With GRE VPNs, a service provider or carrier can outsource their wide area network for transport services. Service providers and carriers do not have to dedicate network elements to a single customer with GRE VPNs. With GRE VPNs, VPN services can be offered to multiple customers who may have overlapping address space. In addition, the characteristics of GRE enable quicker provisioning of GRE VPNs with lower administrative and support costs. For example, the administrative costs of adding a new network element or new VPN are low.

[0020] Moreover, dynamically establishing GRE VPNs provides security since 1) resource consumption upon detection of an unknown key is limited to a database query and state information and; 2) a hostile attack must spoof the source and destination addresses of the GRE tunnel and guess the key for the VPN. Security can be enhanced by ensuring that an unknown key packet originates from an interior source and not an exterior source. One method for implementing the enhancement would be to look up the source address of the packet in a routing table and ensuring that the route to the source address is 1) known, 2) not the default, and 3) learned via a network update protocol, such as the interior gateway protocol (IGP).

[0021] Figure 2 is a diagram illustrating the network element 105 according to one embodiment of the invention. The network element illustrated in Figure 2 could be the network element 105 or 109. In Figure 2, a control engine 201 is coupled with a forwarding engine 203. The control engine 201 performs the queries for the GRE tunnel attributes and VPN information. The forwarding engine 203 hosts virtual routers including the virtual routers 115, 117, and 119. The forwarding engine 203 is coupled

with input/output modules 205A – 205X. The I/O modules 205A – 205X process traffic to be transmitted and process traffic that has been received.

[0022] The control engine 201 and the forwarding engine 203 illustrated in Figure 2 include memories, processors, and/or Application Specific Integrated Circuit ("ASICs"). Such memories include a machine-readable medium on which is stored a set of instructions (i.e., software) embodying any one, or all, of the methodologies described herein. Software can reside, completely or at least partially, within this memory and/or within the processor and/or ASICs. For the purpose of this specification, the term "machine-readable medium" shall be taken to include any mechanism that provides (i.e., stores and/or transmits) information in a form readable by a machine (e.g., a computer). For example, a machine-readable medium includes read only memory ("ROM"), random access memory ("RAM"), magnetic disk storage media, optical storage media, flash memory devices, electrical, optical, acoustical, or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.), etc.

[0023] While the invention has been described in terms of several embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. For example, keys can be defined globally or regionally. In an embodiment of the present invention, regional keys are used in conjunction with regional indicators to identify a VPN. In another embodiment of the present invention, a tunnel is provisioned for each VPN. In another embodiment of the present invention, multiple VPNs are provisioned for a tunnel.

[0024] The method and apparatus of the invention can be practiced with modification and alteration within the spirit and scope of the appended claims. For example, the present invention can be implemented with another tunneling protocol similar to GRE. The description is thus to be regarded as illustrative instead of limiting on the invention.